BDO USA

ARTICLE

October 19, 2023

Rethinking Network Security: Why Zero Trust is the Future, and VPNs are the Past

In the ever-evolving world of cybersecurity, organizations are constantly seeking more effective ways to protect their sensitive data and digital assets. One of the most significant paradigm shifts in recent years has been the move away from traditional Virtual Private Networks (VPNs) in favor of a more advanced approach known as Zero Trust Network Access (ZTNA). In this article, we explore the reasons why organizations should embrace this transformative shift towards Zero Trust, leaving VPNs in the rearview mirror.

The Vulnerabilities of VPNs

Historically, VPNs have been the go-to solution for remote access and secure connectivity. However, recent high-profile breaches have exposed significant vulnerabilities in this traditional

model. Notable breaches such as the 2020 SolarWinds attack and the 2017 Equifax breach both had VPNs as a common entry point for attackers.

1. Limited Access Control

VPNs typically provide users with network access once they've successfully authenticated. Once inside, users often have broad access to resources, making it challenging to limit their movement within the network. Attackers who gain access to a VPN can move laterally, increasing the risk of data breaches and espionage.

2. Single-Point-of-Entry

VPNs rely on a single point of entry, making them a prime target for attackers. A successful breach at this entry point can lead to unrestricted access to an organization's network and data, as seen in the SolarWinds breach.

3. Complex Configuration

VPNs can be complex to set up and manage, often requiring dedicated IT resources. As technology has evolved, the maintenance and configuration demands have grown, making them more susceptible to misconfigurations that can be exploited by cybercriminals.

Enter Zero Trust Network Access (ZTNA)

The Zero Trust model, on the other hand, assumes that no one, whether inside or outside the organization, can be trusted by default. It enforces strict access controls and verifies every user, device, and application attempting to connect to the network. Here's why ZTNA is the way forward:

1. Granular Access Control

ZTNA solutions provide organizations with granular access controls. Users are only granted access to the specific resources they need to perform their job, reducing the attack surface and limiting lateral movement for potential attackers.

2. Continuous Verification

Unlike VPNs that authenticate users once and grant them access, ZTNA solutions continuously verify the trustworthiness of users and devices throughout their session. This proactive approach helps detect and mitigate threats in real-time.

3. Application-Centric Security

ZTNA focuses on securing applications rather than the network itself. This is particularly relevant in today's cloud-centric world, where applications are no longer confined to on-premises servers.

ZTNA can secure access to cloud-based resources with ease.

4. Simplicity and Scalability

Implementing ZTNA can be more straightforward and scalable compared to managing and maintaining complex VPN configurations. It aligns well with modern workforces that are increasingly remote and mobile.

Embracing the Future

As organizations adapt to the evolving threat landscape, they must prioritize a proactive, comprehensive security approach. The shift from VPNs to Zero Trust Network Access represents a significant step in this direction. By leaving the vulnerabilities of VPNs behind and adopting the principles of Zero Trust, organizations can enhance their cybersecurity posture, reduce the risk of breaches, and safeguard their most valuable assets.

In conclusion, VPNs, once a stalwart of remote connectivity, are no longer sufficient to protect against modern cyber threats. The move towards Zero Trust Network Access is a critical step in securing the future of organizations. It's time to embrace this transformative approach and leave the vulnerabilities of VPNs in the past.

Interested in implementing a comprehensive managed cybersecurity solution, but not sure where to start?

BDO Digital is offering a 30-minute consultation to answer your business's cybersecurity and managed IT security services questions and advise on next steps at no cost to your organization for qualifying companies.

Request Free Consultation